UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/507,190	09/09/2004	Pim Theo Tuyls	NL 020192	1803

24737 7590 12/30/2008
PHILIPS INTELLECTUAL PROPERTY & STANDARDS
P.O. BOX 3001
BRIARCLIFF MANOR, NY 10510

EXAMINER	
TRAORE, FATOUMATA	
ART UNIT	PAPER NUMBER
2436	
MAIL DATE	DELIVERY MODE
12/30/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/507,190	TUYLS ET AL.	
	Examiner	Art Unit	
	FATOUMATA TRAORE	2436	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 October 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *14,9-20* is/are rejected.

7)☐ Claim(s) *5-8* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response of the appeal brief filing of April 7, 2008. Claims 1-21, 23-38 are pending and have been considered below.

2. In view of the appeal brief filed on 04/07/2008, PROSECUTION IS HEREBY REOPENED. A new ground of rejection is set forth below.

a. To avoid abandonment of the application, appellant must exercise one of the following two options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final)or a reply under 37 CFR 1.113 (if this Office action is final); or,

(2) initiate a new appeal by filing a notice of appeal under 37 CFR 41.31 followed by an appeal brief under 37 CFR 41.37. The previously paid notice of appeal fee and appeal brief fee can be applied to the new appeal. If, however, the appeal fees set forth in 37 CFR 41.20 have been increased since they were previously paid, then appellant must pay the difference between the increased fees and the amount previously paid.

b. A Supervisory Patent Examiner (SPE) has approved of reopening prosecution by signing below. /Nasser G Moazzami/

Claim Objections

3. Claims 1-20 are objected to because of the following informalities: the different elements of the claim are not on an indented form (see MPEP 608.01(m)). Appropriate correction is required.

Claim Rejections - 35 USC § 101

4. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claim 17 rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

An example of device claim that would not qualify as a statutory process would be a claim that recited purely mental steps. Thus, to qualify as a § 101 statutory process, the claim should positively recite the particular machine to which it is tied, for example by identifying the physical elements that which constitutes the device for example by identifying the physical component of the device to accomplish the step of the claim.

Here, applicant's method steps are not tied to a particular device . Thus, the claim is non-statutory.

The mere recitation of the device in the preamble with an absence of a device in the body of the claim fails to make the claim statutory under 35 USC 101. *Note the Board of Patent Appeals Informative Opinion Ex parte Langemyer et al.*

Double Patenting

5. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

c. A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

d. Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

6. Claim 1 is rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claim 1 of U.S. Patent No. 11,576,354. Although the conflicting claims are not identical, they are not patentably distinct from each other because claim 1 of application number 11,576,354 contains every element of claim 1 of the present application. This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented. A comparison of the claims language in the present application and co-pending application is given below:

10,507,190	11,576,354
1.A method of generating a common secret between a first party and a second party, in which the first party holds a value pI and a symmetrical polynomial P(x, y) fixed in the first argument by the value p~, and the first party performs the steps of sending the value P1 to the second party, receiving a value P2 from the second party and calculating the common secret Si by evaluating the polynomial P(X, Y) in P2, characterized in that the first party additionally holds a value q1 and a symmetrical polynomial Q(x, z) fixed in the first argument by the value q~, and further performs the steps of sending q1 to the second party, receiving a value q2 from the second party and calculating the secret S1 as	1.A method of generating a common secret between a first device A (701) and a second different device B (702), comprising the steps of: pre-distributing (201) (301) (401) (501) to said first and second device a respective secret unique identity xA x1 and 8 Xi+I ~ " " " ~ XK and, based on a master polynomial p(x~ ....,xk) : GF(q)k ~ GF(q), respective secret polynomial in multiple variables qA (Y,+, ...Yk) = p(xA,"", X~, Yi+~ ..... Yk) and XB q,(Y~, Y,) = P(Y,,...,Y,, i+~,..., K) Where XB qA(i+I,'",xk) = qe(xI ..... xi); exchanging (202) (203) (302) said unique identity by at least one of said first device with said second device (402) (502) and

Sr-Q(qb q2)-P(pb p2)	*said second device with said first device; and computing (204) (205) (304) (305) (403) (405) (503) (505)by each said first and second device with their respective secret polynomials a common secret key as:* *KA,B xBx = qA(x,+,,...,x,) = qs(x~,...,x;) = p(x~,...,x, ,x,+,,..., k).*

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 1, 9-12,and 16-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Herzberg et al (US 5,202,921) in view of Hoffstein et al (US 6,076,163).

Claims 1, 16, 17 and 19:Herzberg et al discloses a method, a system , a device and a computer program product of generating a common secret between a first party and a second party(abstract; column 2, lines 45-60; column 3 lines 20-40),

in which the first party holds a value P1 and a symmetrical polynomial P(x, y) fixed in the first argument by the value p1, and the first party performs the steps of sending the value p1to the second party, receiving a value P2 from the second party and calculating the common secret S1 by evaluating the polynomial P(p1, y) in P2(column5, line 60 to column7 line26) , but does not explicitly discloses characterized in that the first party additionally holds a value q1 and a symmetrical polynomial Q(x, z) fixed in the first argument by the value q1 and further performs the steps of sending q1 to the second party, receiving a value q2 from the second party and calculating the secret S1 as S1=Q(q1, q2).P(P1, P2). , but does not explicitly discloses that the secret is generated based on the product of two symmetrical polynomial. However, Hoffstein et al discloses a secure user identification method, system, device and computer program product, which further discloses a step of generating a secret key based on the product of two symmetrical polynomial(column 3, lines 31-46 and Fig. 3). Therefore, it would have been obvious to one having ordinary skills in the art at the time the invention was made to generate a secret based on a product of two polynomial. One would have been motivated to do so in order to maintain a secure communication by not allowing eavesdroppers to access critical information.

Claim 9: Herzberg et al and Hoffstein et al disclose a method for of generating a private pair of key for enciphering communication between the users as in claim 1 above, and Herzberg et al further discloses that the first party and the second

party use a non-linear function on the generated secret S1 and S2, respectively, before using it as a secret key in further communications (column 5, lines 50-60).

Claim 10: Herzberg et al and Hoffstein et al disclose a method for of generating a private pair of key for enciphering communication between the users as in claim 9 above, and Hoffstein et al further discloses that a one-way hash function is applied to the generated secrets S1 and S2(the above described user identification technique can be converted to a digital signature technique by the prover applying a one way hash function to Ag(x) to generate a simulated challenge polynomial) (column 3, lines 30-46). Therefore, it would have been obvious to one having ordinary skills in the art at the time the invention was made to modify the teaching of Herzberg et al such as to use a hash function. One would have been motivated to do so in order to maintain a secure communication by not allowing eavesdroppers to access critical information.

Claim 11: Herzberg et al and Hoffstein et al disclose a method for generating a private pair of key for enciphering communication between the users as in claim 9 above, and Herzberg et al further discloses that the first party and the second party use a non-linear function on the generated secret S1 and S2, respectively, before using it as a secret key in further communications (column 5, lines 60-65).

Claim 12: Herzberg et al and Hoffstein et al disclose a method for generating a private pair of key for enciphering communication between the users as in claim

1 above, and Herzberg et al further discloses that a step of verifying that the second party knows the secret S1 (column 6, lines 20-35).

Claim 18: Herzberg et al and Hoffstein et al disclose a system for of generating a private pair of key for enciphering communication between the users as in claim 17 above, and Herzberg et al further discloses a storage means for storing the polynomial P and the polynomial Q in the form their respective coefficients (column 5, lines 25-40).

9. Claims 2-4 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Herzberg et al (US 5,202,921) in view of Hoffstein et al (US 6,076,163) in further view of Matyas et al (US 5953420).

Claim 2: Herzberg et al and Hoffstein et al disclose a method for generating a private pair of key for enciphering communication between the users as in claim 1 above, while neither of them exclusive discloses a step of generating random numbers. However, Matyas et al discloses a method for establishing an authenticated shared secret value between a pair of users, which further discloses that the first party further performs the steps of obtaining a random number r1 (user A generates a secret value Xla using a pseudorandom number generator) (column 6, lines 15-20), calculating .r1. q1 (generates a public value Y1 from the secret value Xl as Y1 = G^xl mod p) (column 6 lines 20-25), sending r1 .q1 to the second party(each party transmits its own public value Y1 to the other party) (column 6, lines 35-38), receiving r2.q2 from the second party and calculating the secret S1 as S1=Q(q1, rl.r2.q2).P (pl, p2) (each party generates a

value Z2 from the public value Y2 received from the other party and its own secret value X2.as Z2 =Y2^x2 mod p) (column 7, lines 33-45). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined method of Herzberg et al and Hoffstein et al such as to generate random number in the secret key exchange protocol as taught by Matyas et al. The motivation of doing so would have been against attempts to retrieve the key.

Claim 3: Herzberg et al, Hoffstein et al and Matyas et disclose a method for generating a private pair of key for enciphering communication between the users as in claim 2 above, and Matyas et al further discloses that the first party holds the Value q1 multiplied by an arbitrarily chosen value r (user A generates a secret value Xla using a pseudorandom number generator) (column 6, lines 15-20), and the product Q (q1, z). P (pl, y) instead of the individual polynomials P (pl, y) and Q (q1, z) (generates a public value Y1 from the secret value Xl as Y1 = G^xl mod p) (column 6 lines 20-25), and the first party performs the steps of calculating r1 .r.q1, sending rl.r.q1 to the second party, receiving r2.r.q2 from the second party and calculating the secret S1 as S1= Q (q1, rl.r2.r.q2). P (pl, p2) (each party generates a value Z2 from the public value Y2 received from the other party and its own secret value X2 as Z2 =Y2^x2 mod p) (column 7, lines 33-45). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined method of Herzberg et

al and Hoffstein et al such as to generate a Secret S1 as taught by Matyas et al. The motivation of doing so would have been against attempts to retrieve the key.

Claims 4, and 20: Herzberg et al and Hoffstein et al disclose a method for generating a private pair of key for enciphering communication between the users as in claims 1 and 16 above, while above, while neither of them exclusive discloses a step of generating the secret key S2. However, Matyas et al discloses a method for establishing an authenticated shared secret value between a pair of users, which further discloses that the second party holds a value P2 and a value q2(Fig. 4, item 400), the symmetrical polynomial P(x, y) fixed in the first argument by the value P2, the symmetrical polynomial Q(x, z) fixed in the first argument by the value q2, and the second party performs the steps of sending q2 to the first party(Fig.7 step 706), receiving q1 from the first party (Fig. 7, step 708)and calculating a secret S2 as S2=Q(q2, q1)'P(P2, P1), whereby the common secret has been generated if the secret S2 equals the secret S1(each party generates a value Z2 from the public value Y2 received from the other party and its own secret value X2 as Z2 =Y2^x2 mod p) (column 7, lines 33-45). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined method of Herzberg et al and Hoffstein et al such as to generate a secret S1 as taught by Matyas et al. The motivation of doing so would have been against attempts to retrieve the key.

10. Claims 13-15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Herzberg et al (US 5,202,921) in view of Hoffstein et al (US 6,076,163) in further view of Menezes et al (handbook of applied Cryptography, ISBN 0-8493-8523-7 1997).

Claim 13: Herzberg et al and Hoffstein et al disclose a method for generating a private pair of key for enciphering communication between the users as in claim 12 above, while neither of them explicitly a step of applying a zero knowledge protocol. However, Menezes et al discloses a similar method, which further discloses that the first party subsequently applies a zero-knowledge protocol to verify that the second party knows the secret S1 (The prover claiming to be A selects a random element from pre-defined set as its secret commitment, and from this computes an associated (public) witness. This provides initial randomness for variation from other protocols runs, and essentially defines a set of questions all of which the prove claims to be able to answer, thereby a priori constraining her forthcoming response. By protocol design, only the legitimate party A, with knowledge of A's secret, is truly capable of answering all the questions, and the answer to any one of these provides no information about A's long-term Secret) (pages 409-410, section (IV)). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined method of Leighton et al and Hoffstein et al such as to use a zero-knowledge protocol as taught by Menezes et al. The motivation of doing so would have been providing unconditional security.

Claim 14: Herzberg et al and Hoffstein et al disclose a method for generating a private pair of key for enciphering communication between the users as in claim 12 above, while neither of them explicitly a step of applying a commitment- based protocol and Menezes et al discloses a similar method, which further discloses that the first party subsequently applies a commitment-based protocol to verify that the second party knows the secret S1 (*The prover claiming to be A selects a random element from pre-defined set as its secret commitment, and from this computes an associated (public) witness. This provides initial randomness for variation from other protocols runs, and essentially defines a set of questions all of which the prove claims to be able to answer, thereby a priori constraining her forthcoming response. By protocol design, only the legitimate party A, with knowledge of A's secret, is truly capable of answering all the questions, and the answer to any one of these provides no information about A's long-term secret) (pages 409-410, section (IV)*). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined method of Herzberg et al and Hoffstein et al such that to use a commitment based protocol as taught by Menezes et al. The motivation of doing so would have been providing unconditional security.

Claim 15: Herzberg et al and Hoffstein et al disclose a method for generating a private pair of key for enciphering communication between the users as in claim 14 above, while neither of them explicitly a step of using a symmetric cipher to encrypt a random challenge. However, Menezes et al disclose a similar method

which, further discloses that the second party uses a symmetric cipher to encrypt a random challenge (*b chooses a random r, computes the witness x = h(r) (x demonstrates knowledge of r without disclosing it and computes the challenge e = PA(r, B)) (page 404, section (I))*, and sends the encrypted random challenge to the first party(*B sends the encrypted random challenge to A. A decrypts e to recover r' and B' computes x' = h (r') (page 404, section (I)* and the first party subsequently uses the same symmetric cipher as a commit function to commit himself to a decryption of the encrypted random challenge (*A sends r= r1 to B. B succeeds with unilateral entity authentication of A upon verifying) (page 404, section (I))*. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined method of Herzberg et al and Hoffstein et al such as to use a symmetric cipher as taught by Menezes et al. The motivation of doing so would have been providing unconditional security.

Allowable Subject Matter

11. Claims 5-8 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Fatoumata Traore whose telephone number is (571) 270-1685. The examiner can normally be reached Monday through Thursday from 7:00 a.m. to 4:00 p.m. and every other Friday from 7:30 a.m. to 3:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nassar G. Moazzami, can be reached on (571) 272 4195. The fax phone number for Formal or Official faxes to Technology Center 2100 is (571) 273-8300. Draft or Informal faxes, which will not be entered in the application, may be submitted directly to the examiner at (571) 270-2685.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Group Receptionist whose telephone number is (571) 272-2100.

FT

Friday, December 26, 2008

/Nasser G Moazzami/

Supervisory Patent Examiner, Art Unit 2436